Martín Losada

MARTÍN LOSADA CANEDO

IT CONSULTING DOCUHEALTH

CIBERSEGURIDAD

Introducción

📌Presentamos los resultados de una auditoría realizada a DocuHealth

📌¿Qué veremos?

📌¿Por qué es importante?

DOCUHEALTH

Objetivos de la auditoría

- ✓ Evaluar la seguridad técnica y organizativa
- ✓ Verificar el cumplimiento del RGPD y otras normativas
- ✓ Detectar vulnerabilidades y proponer mejoras
- ✓ Preparar el camino hacia certificaciones como ISO 27001

Martín Losada

Que es DocuHealth?

- Startup tecnológica especializada en telemedicina
- Pacientes particulares y clínicas privadas
- Todo integrado en una infraestructura en la nube

Martín Losada

Introducción al marco normativo aplicable

Norma / Referencia

RGPD (UE) 2016/679

LOPDGDD

ISO/IEC 27001

ENS (Esquema Nacional de Seguridad)

Ley 41/2002

Como aplica cada norma a DocuHealth ?

Martín Losada

Principio de responsabilidad proactiva

El RGPD exige no solo cumplir con las normas, sino poder demostrar que se está cumpliendo.

DocuHealth debe documemtar :

- ✓ Politicas de privacidad.
- ✓ Registros de actividades de tratamiento
- ✓ DPIA si aplica

Clave :

La responsabilidad proactiva es lo que convierte el cumplimiento en un sistema vivo, no en un montón de papeles.

Martín Losada

DOCUHEALTH

Medidas técnicas y organizativas (Art. 32 RGPD)

📌 El Art. 32 exige medidas técnicas y organizativas adecuadas, entre ellas:

✔ Cifrado
✔ Control de accesos
✔ Copias de seguridad
✔ Segmentación de red
✔ Formación de personal

📌 DocuHealth debe combinar herramientas técnicas (, con procedimientos internos

✔ MFA
✔ cifrado de BBDD
✔ Monitorización
✔ Políticas
✔ Roles claros
✔ Respuesta ante incidentes

Martín Losada

DOCUHEALTH

RGPD – Artículos clave aplicables a DocuHealth

Artículo	Tema	Ejemplo aplicado a DocuHealth
Art. 5	Principios del tratamiento	Minimización de datos en formularios de registro.
Art. 6	Licitud del tratamiento	Base legal: ejecución de contrato (consultas), consentimiento explícito (datos de salud).
Art. 9	Datos especialmente protegidos	Historial clínico → requiere condiciones reforzadas.
Art. 25	Protección de datos desde el diseño	MFA, cifrado, roles definidos en los accesos.
Art. 30	Registro de actividades	Mapa de tratamientos con responsables y finalidades.
Art. 32	Seguridad de tratamiento	Medidas técnicas y organizativas eficaces.
Art. 35	Evaluación de Impacto (DPIA)	Obligatoria por tratar datos de salud a gran escala.

¿DocuHealth debe hacer una DPIA?

📌 El Art. 35 exige una DPIA cuando se tratan datos sensibles a gran escala o cuando hay:

- ✓ Evaluación sistemática de personas (historial médico, seguimiento clínico)
- ✓ Observación a distancia (por ejemplo, monitorización continua)

📌 En DocuHealth se dan al menos dos condiciones:

- ✓ Datos de salud → categoría especial
- ✓ Observación a distancia (por ejemplo, monitorización continua)

Martín Losada

DOCUHEALTH

Alcance de la Auditoría

Sistemas y procesos auditados

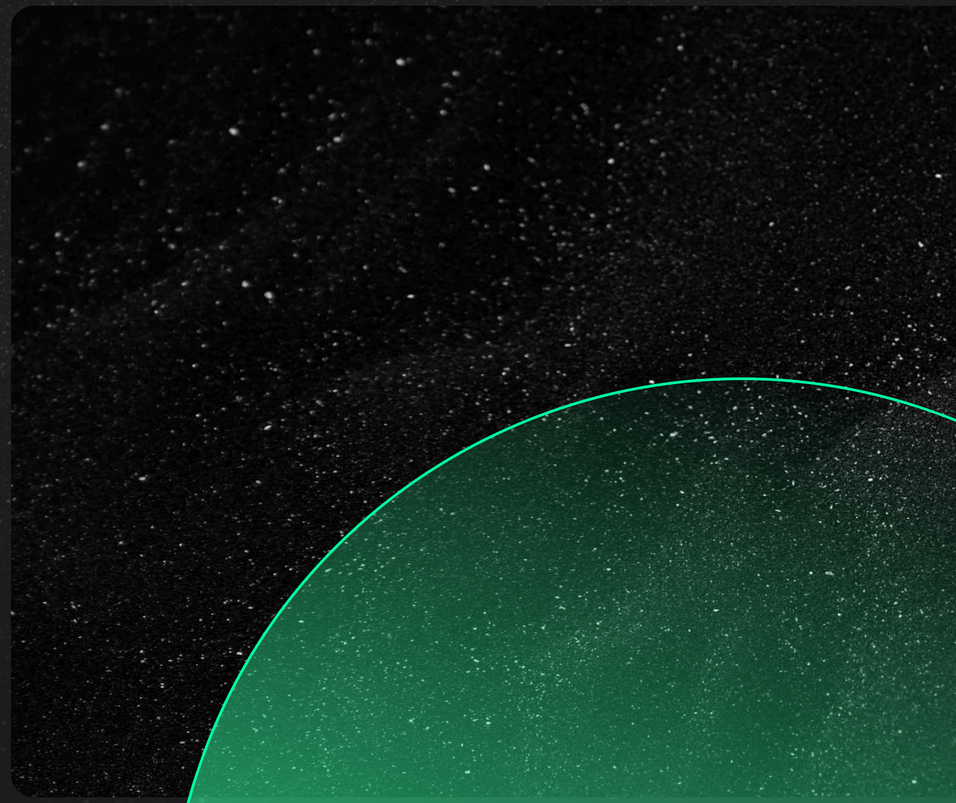
¿Que se ha auditado?

- Plataforma web de acceso para pacientes y médicos
- Aplicaciones móviles (Android / iOS)
- Servidores backend desplegados en la nube (AWS)
- Base de datos con información clínica y personal
- API REST para integraciones externas con clínicas privadas
- Plataforma integrada de videollamadas (WebRTC)
- Pasarela de pagos (Stripe) y sistema de notificaciones (SMS, email)

También se ha revisado el tratamiento de los datos especialmente protegidos (salud), financieros, técnicos y personales.

Martín Losada

Metodología aplicada



La auditoría se ha desarrollado combinando distintas técnicas:

1. **Revisión documental**
Políticas, configuraciones, logs y evidencias de cumplimiento.

2. **Entrevistas clave**
DPO, CISO y DevSecOps para conocer procesos y riesgos.

3. **Análisis técnico**
Seguridad cloud, cifrado, accesos, MFA, backups.

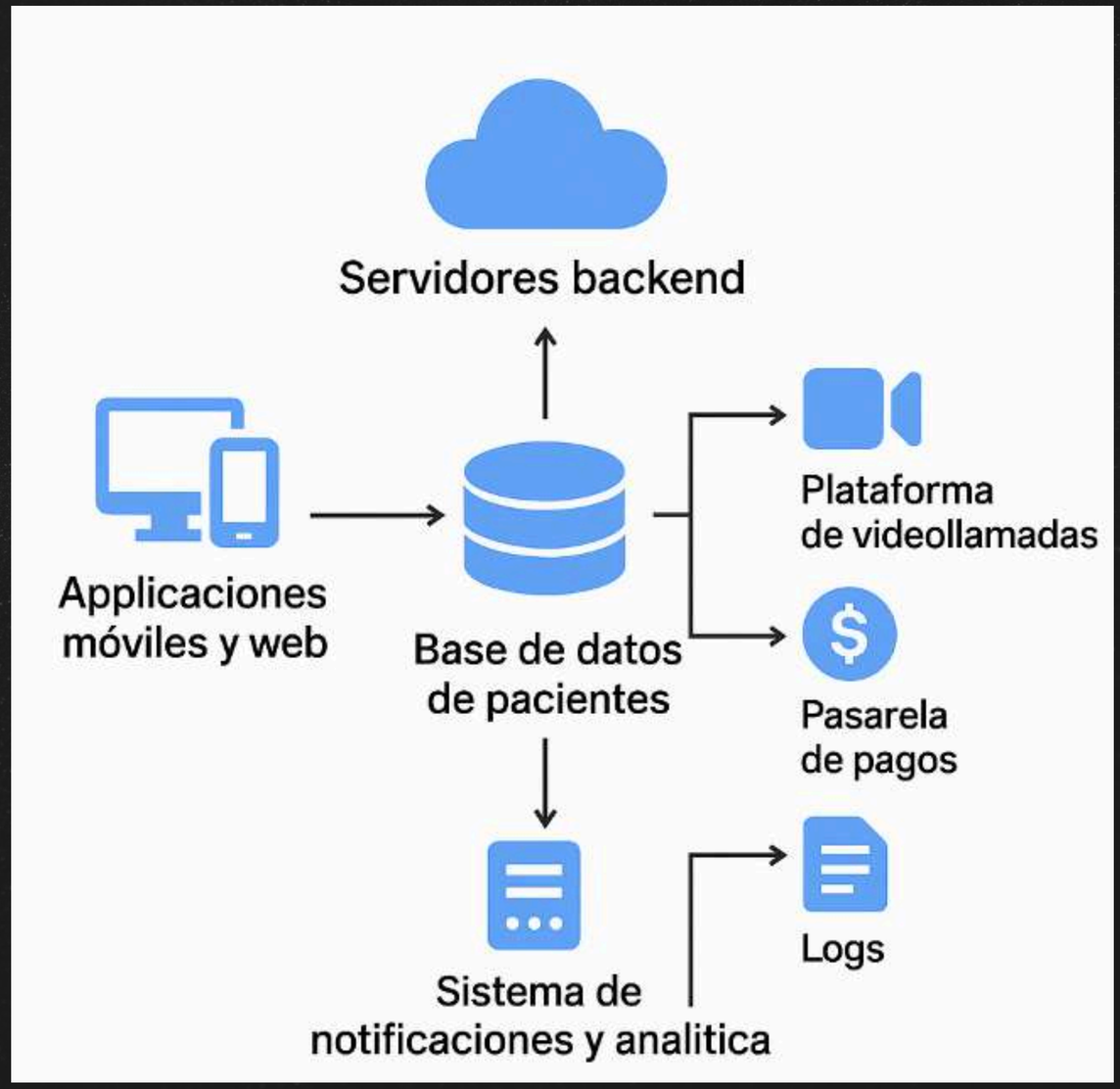
4. **Enfoque normativo**
Evaluación conforme a RGPD, LOPDGDD e ISO 27001 (referencia).

Martín Losada

DOCUHEALTH

Identificación de activos

- Base de datos de pacientes
- Servidores backend desplegados en la nube
- Aplicaciones móviles y web
- Plataforma de videollamadas, pasarela de pago y sistema de notificaciones
- Logs, registros de acceso, geolocalización y metadatos técnicos



Roles clave en la gestión de activos

- El DPO o delegado de protección de datos → **Garantiza que todos los tratamientos de datos se ajustan al RGPD**
- El CISO o Chief Information Security Officer → **Se encarga de la seguridad de la información** → **Técnicas**, **Gestión de incidentes**
- El CTO o director de tecnología y el equipo de DevSecOps(equipo de desarrollo, seguridad y operaciones) → diseñan, desarrollan y mantienen la infraestructura tecnológica
- Los médicos y personal de soporte → **Acceden diariamente a datos de pacientes y cumplen diferentes protocolos**

Martín Losada

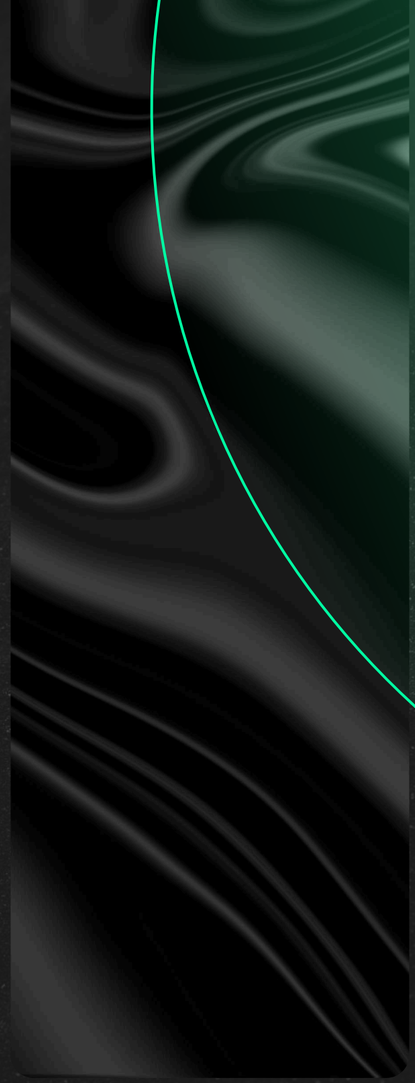
DOCUHEALTH

¿Por qué evaluar riesgos?

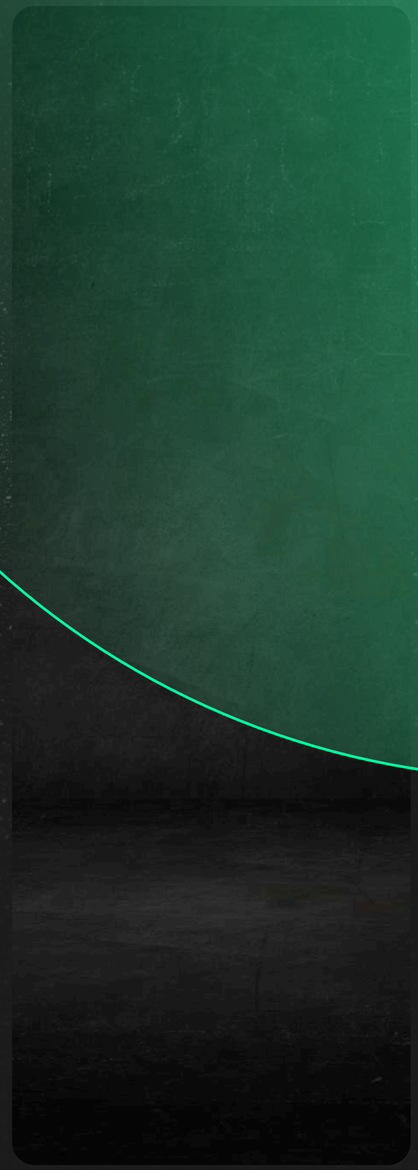
- **DocuHealth trata datos de salud → riesgo alto por naturaleza**
- **El RGPD (Art. 32) exige identificar riesgos y adoptar medidas proporcionales**

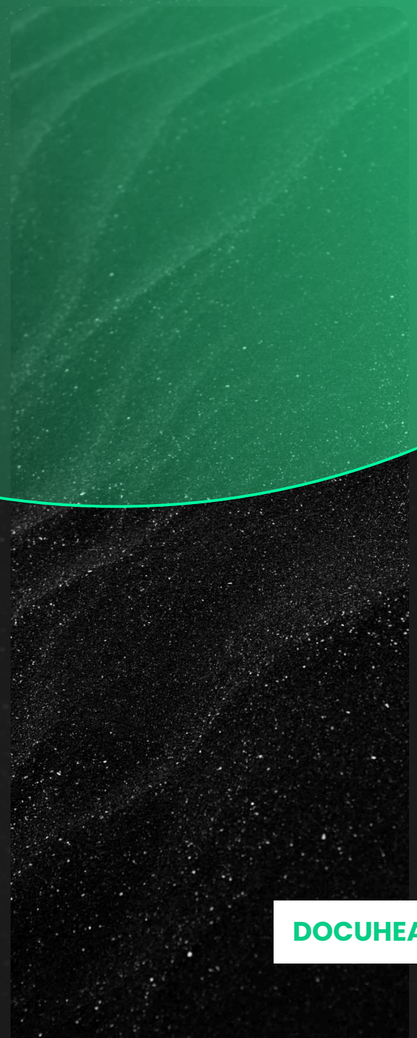
Evaluar riesgos permite:

- ✓ Priorizar medidas
- ✓ Justificar inversiones
- ✓ Cumplir con responsabilidad proactiva



En ciberseguridad, todo se trata de riesgo.
No podemos proteger todo por igual.





Martín Losada

DOCUHEALTH

Metodología simple pero efectiva: Probabilidad × Impacto

Modelo cualitativo

- Probabilidad: ¿Qué tan probable es que ocurra el incidente?
- Impacto: ¿Qué daño causaría si ocurre?
- Se cruzan en una matriz de riesgo

Niveles utilizados:

- Probabilidad: Baja / Media / Alta
- Impacto: Bajo / Medio / Alto
- Resultado: Riesgo Bajo, Medio, Alto o Crítico

Martín Losada

DOCUHEALTH

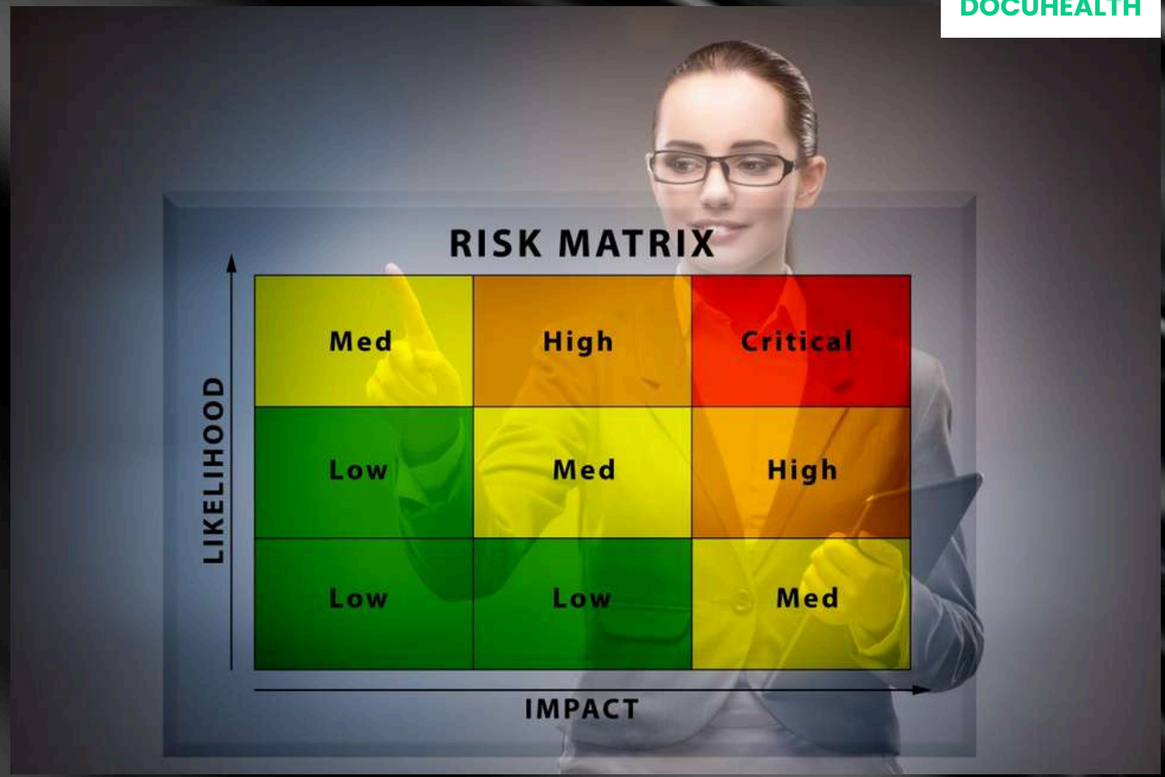
Amenazas reales para una plataforma de salud

Amenaza	¿Por qué preocupa?
Phishing a personal médico	Acceso indebido a historiales clínicos
Configuración insegura en la nube	Fuga masiva de datos de pacientes
Falta de MFA en accesos críticos	Suplantación de identidad
Brechas por terceros (proveedores)	Pasarela de pago o email comprometido
Ausencia de monitorización/logs	No se detecta un acceso ilegal a tiempo

Martín Losada

DOCUHEALTH

Visualizando el riesgo: nuestra matriz de impacto



- Phishing → Probabilidad: Alta / Impacto: Alto → Riesgo Crítico-
- Fallo de backups → Probabilidad: Media / Impacto: Alto → Riesgo Alto
- Filtración por API mal protegida → Media / Medio → Riesgo Medio

Principales hallazgos

📌Principales hallazgos/vulenerabilidades identificadas:

- Sin MFA en accesos de administración y cuentas sensibles
- Backups sin cifrado (ni en reposo ni en tránsito)
- Logs de actividad incompletos
- Permisos de usuario mal gestionados (roles no definidos)
- Contratos con proveedores poco revisados
- Falta de formación en protección de datos para personal no técnico

Martín Losada

DOCUHEALTH

Recomendaciones clave

RECOMENDACIONES

MEDIDAS DE MEJORA

- Activar MFA en accesos críticos y administrativos
- Cifrar backups y datos sensibles, tanto en tránsito como en reposo
- Centralizar logs y habilitar alertas ante actividades anómalas
- Revisar roles y permisos, aplicando el principio de mínimo privilegio
- Auditar proveedores y asegurar cláusulas de seguridad en contratos
- Formación continua para todo el personal en protección de datos

✓ Objetivo:
Reducir el riesgo de brechas de seguridad y fortalecer el cumplimiento de las normativas

Martín Losada

DOCUHEALTH

Martín Losada

DOCUHEALTH

Plan de acción y Roadmap

Después de identificar los activos críticos y sus riesgos asociados se define un **plan de acción**

Corto plazo

- Auditoría interna inicial y análisis de brechas
- Refuerzo de medidas básicas
  - Cifrado
  - Revisión de políticas de acceso
  - Contraseñas
- Formación rápida en RGPD y seguridad para el personal médico y técnico
- Actualización de la política de privacidad y revisión del consentimiento

Martín Losada

DOCUHEALTH

Medio plazo

- Implementación de medidas avanzadas de seguridad
- Revisión y documentación de procedimientos
  - Gestión de incidentes
  - Copias de seguridad
  - Continuidad de negocio
- **Evaluación de proveedores externos, para verificar cumplimiento**

- Primer ejercicio de análisis de riesgos formalizado con el DPO y CISO

Martín Losada

DOCUHEALTH

Largo plazo

- Preparación y posible inicio de certificación ISO 27001
- Integración de auditorías técnicas
- **Automatización de monitorización y generación de informes**
- Consolidación de cultura de seguridad en la organización

Martín Losada

DOCUHEALTH

Seguimiento continuo

- Auditorías internas
- Revisiones semestrales
- Mecanismos de mejora continua

Martín Losada

DOCUHEALTH

Responsables

- DPO, lidera lo relacionado con privacidad y tratamiento de datos
- El CISO, coordina las medidas técnicas y de gestión de riesgo
- **El equipo DevSecOps, clave en la implementación diaria**
- La dirección, apoyará con recursos económicos y prioriza la agenda coorporativa

Martín Losada

DOCUHEALTH

Martín Losada

MUCHAS GRACIAS POR VUESTRA ATENCIÓN

IT Consulting docuhealth

DOCUHEALTH